REMARKS

Claims 1-39 are currently pending in the subject application and are presently under consideration. Claims 1-5, 7-27, 29, 30, 31, and 33-35 have been amended as shown on pages 2-11 of the Reply.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Claim Objections

Claim 1 is objected because of general clarity issues. It is believed that the amendments to claim 1 herein address the Examiner's concerns in this regard. Withdrawal of this objection is therefore respectfully requested.

II. Rejection of Claims 12-17, 19-22, 24, 26-31, 34, and 36-39 Under 35 U.S.C. §102(a)

Claims 12-17, 19-22, 24, 26-31, 34, and 36-39 stand rejected under 35 U.S.C. §102(a) as allegedly being anticipated by Mikami (U.S. 2004/0034799). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Mikami does not disclose or suggest each and every feature set forth in the subject claims.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The subject application relates generally to shared role-specific portal configurations that provide a user with selective access to networked components based on the user's defined role and location. To this end, portal configurations can be generated to provide default and customized portals for respective users. The configurations can be stored local to a portal or on other networked components such as within common and local storage areas, such that the configurations can be shared amongst users with similar roles (see, *e.g.*, paragraph [0009]). To facilitate selection of an appropriate profile for a given operator, a hierarchy or matrix of operator information can be employed to determine the operator's scope (see, *e.g.*, paragraph [0071]). This hierarchy can comprise at least one location-specific configuration (*e.g.*, a building) as a nested portal from a base portal configuration. The location-specific configuration can be associated with a home configuration, an administrative configuration, and a users configuration (see, *e.g.*, paragraphs [0077]-[0079] and Figure 8). After generating such a hierarchical architecture, this architecture can be loaded and utilized, or saved in a common storage location for later employment. When a user logs on to a portal, the logon information can be utilized to locate the operator's role from the hierarchy in order to provide the user with access to components based on the user's role (see, *e.g.*, paragraph [0084]). In particular, amended independent claim 12 recites, ***a role hierarchy that defines a plurality of user roles and associated access privileges and organizes the plurality of user roles according to location****; a profile bank configured to store a plurality of portal configurations that respectively define one or more network components to which access is allowed, wherein* ***at least one of the plurality of portal configurations has a defined association with at least one of the plurality of user roles and at least one location****; and a loading component configured to* ***access the role hierarchy upon receiving a login notification to determine a login user role and a login user location associated with the login notification, and to launch at least one selected portal configuration of the plurality of portal configurations based on the login user role and the login user location****.*

Mikami does not disclose or suggest at least these aspects. Mikami relates to a system that allows user profile information defining Web contents to be display to be shared between users. According to this system, profile information on Web applications set by individual users is recorded a storage device of a portal server. Permission to use part of a user's personal profile information is given from one user to another in order to share part of the profile information about particular portal applications (see paragraph [0029]). If a second user receives permission from a first user to use the first user's portal page, the second user's attribute information is merged with the first user's attribute information, and the portal server selects portal applications according to this merged profile information when the second user logs in to the ISP. Using the merged profile information, a portal page is constructed containing the portal page for the second user and a portal application menu having applications that the first user has permitted the second user to use (see paragraph [0036]).

However, Mikami does not contemplate the use of a *role hierarchy* defining a plurality of user roles and associated privileges that are organized according to location, and in particular fails to disclose accessing such a hierarchy to determine a login user role and a login user location associated with a login. Indeed, the portal profiles described in Mikami are neither role-specific nor location-specific. Rather, Mikami's portal profiles are associated only with the respective *individuals* to whom the portal profiles are assigned, and it is nowhere disclosed in the cited reference that a portal configuration presented to a user can be associated with a particular user role or user location. Consequently, there is no motivation within Mikami to include a mechanism for identifying a user role and location in response to a login notification. The cited reference therefore fails to disclose or suggest the architecture and functionality of the role hierarchy of amended independent claim 12.

Similarly, amended independent claim 21 recites, ***configuring a role hierarchy defining a plurality of locations and user roles associated with the respective plurality of locations;*** *storing a plurality of portal configurations defining respective one or more network components to which access is allowed;* ***associating at least one of the plurality of portal configurations with at least one of the user roles and at least one of the plurality of locations;*** *logging in under a user identity;* ***accessing the role hierarchy to determine a login user role and a login user location associated with the user identity;*** *[and] selecting a selected portal configuration associated with the login user role and the login user location.* Mikami is silent regarding at least these aspects, as discusses *supra.*

Likewise, amended independent claim 26 recites, *logging on to a portal under a user identity;* ***accessing a role hierarchy defining a plurality of locations and respective user roles associated with the respective plurality of locations to determine a login user role and a login user location associated with the user identity;*** *[and] initializing a portal configuration associated with the login user role and the login user location that utilizes one or more portlets to provide selective access to networked components.* As discussed above, the cited reference does not disclose or suggest these features.

In a related aspect, amended independent claim 26 goes on to recite, *filtering a list of available networked components based on the login user role and the login user location to yield a role-specific list of networked components; [and] providing the role-specific list of networked components associated with the login user role and the login user location.* Arguing that

Mikami anticipates these features, the Office Action states that, according to Mikami, "only parentally allowed related attributes are merged with the child profile." Ostensibly, the Examiner is noting that a given user is presented only with those portal applications that are either associated with that user's profile or that have been granted to the user by another user, and attempts to draw a parallel between this selective presentation of portal applications and the act of filtering a list of available network components based on a user's role. However, the parentally allowed attributes indicated in the Office Action are not a function of a *user's role*, but rather represent attributes that have been selected by the parent user for use by the child user. Moreover, as noted above, these parentally allowed attributes are not a function of a *location* associated with a user, and indeed location is not taken into consideration by Mikami when determining a portal configuration to be used by an operator.

Also, amended independent claim 34 recites, *instructions for* ***referencing a hierarchy of locations and associated user roles to determine a login user location and a login user role associated with a user identity****; instructions for instantiating a portal configuration associated with the login user location and the login user role*. The cited reference is silent regarding these aspects, as noted *supra*.

In addition to the features discussed above, one or more embodiments of the present application can allow a customized portal configuration to be saved to local memory or a common storage area. The saved configuration can be associated with an attribute rendering the configuration sharable with other users, such as users with a similar role (see, *e.g.*, paragraph [0053]). In particular, amended claim 15 recites, *the utility allows an attribute to be defined for the at least one modified portal configuration that* ***determines whether the at least one modified portal configuration is to be accessible from the profile bank by other logins associated with the login user role***.

With regard to these aspects, the Office Action notes that Mikami includes a portal application data hiding function, which allows a parent user to select which portal applications associated with the parent user are to be hidden from view on a child user's portal page (paragraph [0066]). However, this hiding function represents a *user-to-user* permissive, in that the hiding function is employed by the parent user to define whether a *selected user* is allowed to view and employ a particular portal application. This hiding function is not described as determining whether *users having a particular login user role* are allowed to access the application. Moreover, since Mikami does not consider a user's *role* in any sense when determining an appropriate portal configuration to be presented to the user, there is no suggestion in the cited reference to employ an attribute determining whether a modified portal configuration is to be accessible via a login *associated with a particular user role.*

Also, according to one or more embodiments, the portals of the present application can allow an operator to associate a portlet with a networked component from a set of networked components available to the operator, wherein the set can be based on the operator's job position (see, *e.g.*, paragraph [0072]). In particular, amended claim 16 recites, *the at least one selected portal configuration renders a subset of network components associated with the login user role, and allows a selected component from the subset of network components to be manually associated with a portlet within the portal to allow access to the selected component.* As noted above, Mikami does not consider a user's role in any way when providing a portal configuration to a user. The cited reference therefore also fails to disclose or suggest rendering a subset of network components *associated with a particular role* to a user to allow manual association of components from this role-specific subset with respective portlets.

In another aspect according to one or more embodiments, more than one instance of a portal configuration can be concurrently instantiated in connection with different portals by users with a similar role (see, *e.g.*, paragraph [0009]). A change to a configuration being shared can be reflected in one or more of the other instances. For example, a user can determine that a portal should be updated or refreshed with the modified configuration when the configuration is saved (see, *e.g.*, paragraph [0050]). In particular, amended claim 19 recites, *at least a first of the multiple instances of the at least one selected portal configuration is dynamically refreshed in response to and in accordance with a modification to at least a second of the multiple instances of the at least one selected portal configuration.*

Asserting that Mikami discloses dynamically refreshing an instance of a portal configuration in response to a change to another instance of the configuration, the Office Action indicates a portion of the cited reference detailing how a parent user can change stored profile information relating to portal applications that can be used by a child user (paragraph [0087]). However, although this paragraph discloses in general that profile information can be modified, it is noted that this procedure is described in the context of performing such a change *prior to running an instance of the portal* defined by the profile information. As such, Mikami does not describe making the indicated profile modifications *as an instance of the associated portal is running*. It therefore cannot be said that the indicated portion of Mikami discloses or suggest dynamically *refreshing a first instance of a portal configuration* in response to a modification made to a *second instance of the portal configuration*.

Moreover, amended claim 22 recites, *the selected portal configuration selected from a set of shared configurations that are associated with the login user role*. Although the Office Action asserts that the sharing of portal page attributes between a parent user and a child user, as described in Mikami, reads on these aspects, it is noted that the cited reference does not indicate that these shared portal page attributes are in any way associated with a particular *user role*. Rather, as discussed above, the shared attributes merely represent attributes selected by the parent user for visibility by the child user. These attributes are not selected from a set of shared configurations associated with a particular *login user role*.

In view of at least the foregoing, it is respectfully submitted that Mikami does not disclose or suggest each and every feature of amended independent claims 12, 21, 26, and 34 (and all claims depending there from), and as such fails to anticipate or render obvious the present application. It is therefore requested that this rejection be withdrawn.

III. <u>Rejection of Claims 1-4, 7, 9-11, 33, and 35 Under 35 U.S.C. §103(a)</u>

Claims 1-4, 7, 9-11, 33, and 35 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Mikami in view of Cook, *et al.* (U.S. 2003/0117437). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Mikami and Cook, *et al.*, individually or in combination, do not disclose or suggest all aspects of the subject claims.

> To reject claims in an application under § 103, an examiner must establish a prima facie case of obviousness. A prima facie case of obviousness is established by a showing of three basic criteria. First, there must be some apparent reason to combine the known elements in the fashion claimed by the patent at issue (*e.g.*, in the references themselves, interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, or in the knowledge generally available to one of ordinary skill in the art). To facilitate review, this analysis should be made explicit. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when

> combined) must teach or suggest all the claim limitations. See MPEP § 706.02(j). See also KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398, 04-1350, slip op. at 14 (2007). The reasonable expectation of success must be found in the prior art and not based on applicant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)

Amended independent claim 1 recites, ***a role hierarchy that defines multiple locations and associated user roles****; a retrieval component configured to* ***access the role hierarchy to identify a login user role and a login user location associated with a login identity and to obtain a selected shared access profile associated with the login user role and the login user location*** *from the one or more shared access profiles stored on the storage component.* As discussed in the previous section of the Reply, Mikami fails to disclose or suggest the use of a role hierarchy to select a shared access profile in this manner. Cook, *et al.* is also silent regarding these features. Cook, *et al.* relates to a portal administration tool that allows group and portal administration tasks to be delegated to selected users. However, Cook, *et al.* does not contemplate the structure or functionality of the role hierarchy set forth in amended independent claim 1. Although Figure 2 of Cook, *et al.* depicts a Group Hierarchy configuration page, this group hierarchy is not used to *select an appropriate shared access profile* in accordance with a user role and a user location associated with a user identity. Rather, this group hierarchy is used only to register users within a particular group (*e.g.*, portal administrator, group administrator, *etc.*) in order to establish that user's administrative rights (see, *e.g.*, paragraphs [0029]-[0040]). Cook, *et al.* does not indicate that this group hierarchy is referenced to determine a particular portal profile to be provided to a given user. Moreover, the group hierarchy depicted in Figure 2 of the cited reference does not define multiple *locations* and their associated user roles, as set forth in amended independent claim 1, but rather only defines user groups to which a user can be added.

Similarly, amended independent claim 33 recites, *means for defining a plurality of locations and respective user roles associated with the plurality of locations in a hierarchical architecture; means for referencing the means for defining to determine a login user role and a login user location associated with a user identity; [and] means for selecting a shared portal configuration providing customized access to the components from one or more configurations* *associated with the login user role and the login user location*. Neither Mikami nor Cook, *et al.* disclose or suggest these features, as discussed *supra*.

Also, amended claim 35 depends from amended independent claim 34, and Cook, *et al.* does not cure the shortcomings of Mikami with regard to *referencing a hierarchy of locations and associated user roles to determine a login user location and a login user role associated with a user identity*, as recited in that independent claim as amended.

In view of at least the foregoing, it is respectfully submitted that Mikami and Cook, *et al.*, individually or in combination, do not disclose or suggest all features of amended independent claims 1, 33, and 34 (and all claims depending there from), and as such fail to make obvious the present application. It is therefore requested that this rejection be withdrawn.

IV. Rejection of Claims 5 and 6 Under 35 U.S.C. §103(a)

Claims 5 and 6 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Mikami in view of Cook, *et al.*, and further in view of Hayes Jr., *et al.* (U.S. 2001/0011341) and Nielsen (U.S. 5,813,007). However claims 5 and 6 depend from amended independent claim 1, and as discussed above in connection with that independent claim, neither Mikami nor Cook, *et al.* disclose or suggest accessing *a role hierarchy that defines multiple locations and associated user roles to identify a login user role and a login user location*, and *obtaining a selected shared access profile associated with the login user role and the login user location.* Hayes, Jr., which relates to a system that manages which applications a given user is permitted to access, is also silent regarding the use of such a role hierarchy. Nielson also fails to cure these deficiencies, since that cited reference merely relates to generation of notifications upon detection of significant changes to the content of a bookmarked web page, and does not contemplate the use of a role hierarchy having the architecture and function set forth in amended independent claim 1.

In view of at least the foregoing, it is respectfully submitted that Mikami, Cook, *et al.*, Hayes, *et al.*, and Nielson, individually or in combination, do not disclose or suggest all aspects of amended independent claim 1. It is therefore requested that this rejection be withdrawn with respect to claims 5 and 6, which depend from that independent claim.

V. Rejection of Claim 8 Under 35 U.S.C. §103(a)

Claim 8 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Mikami in view of Cook, *et al.*, further in view of Abbott, *et al.* (U.S. 2002/0087525). However, claim 8 depends from amended independent claim 1, and as discussed *supra*, Mikami and Cook, *et al.* are silent with regard to *a role hierarchy that defines multiple locations and associated user roles to identify a login user role and a login user location*, and *obtaining a selected shared access profile associated with the login user role and the login user location*. Abbott, *et al.* does not make up these deficiencies. Abbott, *et al.* relates to an information searching system that combines a user search request with context information associated with the user, and employs the combined information to generate search criteria corresponding to the search request. However, this search technique does not involve the use of a role hierarchy having the architecture recited in amended independent claim 1. Indeed, Abbott, *et al.* does not relate to selection and presentation of shared portal profiles in general, and as such fails to contemplate the use of a role hierarchy to identify an appropriate portal profile in accordance with a user's role and location.

In view of at least the foregoing, withdrawal of this rejection is respectfully requested.

VI. Rejection of Claim 23 Under 35 U.S.C. §103(a)

Claim 23 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Mikami in view of Hayes Jr. *et al.* However, amended claim 23 depends from amended independent claim 21, and as discussed above, neither of these references disclose or suggest configuring a *role hierarchy defining a plurality of locations and user roles associated with the respective plurality of locations*, and accessing this role hierarchy to determine a login user role and a login user location associated with the user identity in order to select a portal configuration, as set forth in that independent claim as amended. Withdrawal of this rejection is therefore respectfully requested.

VII. Rejection of Claims 18, 25, and 32 Under 35 U.S.C. §103(a)

Claims 18, 25, and 32 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Mikami in view of Sheppard (U.S. 6,026,397). However, claims 18, 25, and 32 depend from amended independent claims 12, 21, and 26. As discussed *supra*, none of

Mikami, Cook, *et al.*, Hayes, Jr., *et al.*, Nielson, or Abbott, *et al.* disclose the architecture and functionality of the role hierarchy set forth in those independent claims. Sheppard, which relates to techniques for segmenting and clustering data records to facilitate efficient storage in a database, does not remedy the deficiencies of the other cited references in this regard. It is therefore respectfully requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP318US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact Applicant's undersigned representative at the telephone number below.

Respectfully submitted,
TUROCY & WATSON, LLP

/Brian Steed/
Brian Steed
Reg. No. 64,095

TUROCY & WATSON, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731